

3 INTEGRATING SAFETY AND QUALITY IN PROJECTS

3.1 OVERVIEW

The basic approach to project management is to begin the project with the product clearly in mind. This approach includes preparing, early in the project, to consider and identify at least minimal safety, health, environmental, and quality concerns.

3.2 INTEGRATED SAFETY MANAGEMENT

An Integrated Safety Management System (ISMS) is an overall management system designed to ensure that environmental protection and worker and public safety are appropriately addressed in the performance of any task. The fundamental premise of Integrated Safety Management (ISM) is that accidents are preventable through early and close attention to safety, design, and operation, with substantial stakeholder involvement with the teams that plan and execute the project, based on appropriate standards. The safety management system consists of (1) the objective, (2) the guiding principles, (3) the core functions, (4) the mechanisms of implementation, (5) clear responsibilities for implementation, and (6) implementation. As such, an ISMS is characterized by a management system's ability to implement the five core management functions and seven guiding principles using the key implementing factors.

Although safety is a line management function, all members of the Integrated Project Team (IPT) need to maintain a safety focus. In the design stages of a project it is most critical that a safety-through-design approach be embraced. A facility that meets the requirements is not necessarily the safest facility. As will be discussed in the following sections, a safety-through-design approach often permits radical solutions to providing safety that can lead to hazard elimination or reduction by modifications in the process approach or design approach. As noted in Section 3 of the manual, this approach makes use of the familiar ISM principles and functions to address design as well as performing physical work.

3.2.1 Summary

Section 3 of the manual provides the overall description of ISMS and its integration into the project requirements and programs. This Practice will focus on the specifics of implementation at each project stage and the documents that are applicable for that stage. It has been developed with a focus on high-hazard, complex nuclear facilities. Risk based tailoring of the guidance provided within these Practices should include project, public, worker and environmental risks. An ISMS provides an appropriate and effective umbrella for cost-effective implementation of many related DOE programs. For example, safety, health, environmental, and quality issues are best implemented via ISM. The ISMS would not perform its function however as a standalone activity. Therefore, to integrate these principles and functions into the project, they are best defined and implemented via the Project Execution Plan. By integrating ISM into the Project Execution Plan, the implementation of these programs becomes integrated into the project rather than being viewed as a standalone program.

To implement ISM, the project needs to have a commitment to a standards-based safety program. Therefore, the S/RID or work smart standards processes should be an integral part of the first element (Define the Scope of Work) of ISM. As discussed later, the elements of other safety programs, such as Voluntary Protection Program (VPP) and Enhanced Work Planning (EWP), can also be described in terms of the ISM core functions and integrated into the project practices. If the project chooses to implement environmental management via ISO 14001, then the environmental management system elements of ISO 14001 can also be described and implemented through ISM. Environmental management cycle implementation is described in Section 3.4 of this Practice.

A successful ISMS can demonstrate that the implementing documentation and procedures appropriately address the ISMS principles and core functions. A crosswalk of project documentation covering ISM core functions and principles (Figure 3-1) provides a useful tool in both evaluating required project documentation and critical content for specific documents.

3.2.2 ISMS Description

The expectations for an integrated safety management approach can be described by a successive set of actions or activities. This management system is modeled by the five core safety management functions:

	Line Management Responsibility for Safety	Clear Roles and Responsibilities	Competence Commensurate with Responsibilities	Balanced Priorities	Identification of Safety Standards and Requirements	Hazard Controls Tailored to Work Being Performed	Operations Authorization
Baseline Scope of Work	CDR	CDR, QAP, PCS	QAPP	PCS, RP	CDR	SIP	PEP, PCS
Analyze Potential Hazards	CDR, SEMP, DEP	SIP, RMP, PEP	QAPP, SEMP, DEP	CTP, SIP, RMP, SIP	CDR, SIP	SIP	PEP
Develop Design Controls	CMP, SEMP, DEP, ECP	QAPP, PEP, SEMP, DEP, ECP	QAPP	SIP, ECP, SEMP, DEP	SIP, ECP, QAPP	SIP, ECP	OMP, ECP
Perform Work/Design (Planning)	CMP, PMP	QAPP, SEMP	Project Programs and Procedures are Mapped to ISM Design Phase Principles and Core Functions.				
Review, Feedback, Improvement & Validation	QAPP, SEMP	QAPP	QAPP	CDR-Trade Studies, SEMP	QAPP, SEMP	QAPP	RMP, PMP

Nomenclature

Project Execution Plan (PEP)
Project Control System (PCS)
Environmental Compliance Plan (ECP)
Risk Management Plan (RMP)
Design Execution Plan (DEP)
EResource Plan (RP)

Core Technology Plan (CTP)
Safety Implementation Plan (SIP)
Systems Engineering Management Plan (SEMP)
Quality Assurance Program Plan (QAPP)
Project Management Plan (PMP)

Figure 3-1 Typical Crosswalk of ISMS Design Phase Principles and Core Functions

- ▶ Define the work scope and how it is to be prioritized and accomplished.
- ▶ Identify and analyze the hazards associated with the work or eventual use of the design.
- ▶ Develop the controls (including requirements) tailored to the work and hazards.
- ▶ Perform the work as authorized, following confirmation of readiness.
- ▶ Assess the effectiveness of the system and feedback results to improve the process or design.

The five core ISMS functions are usually depicted graphically as shown in Figure 3-2. Although arrows indicate a general direction, these are not independent, sequential functions. They are a linked, interdependent collection of activities that may occur simultaneously. Outcomes during the accomplishment of one function may affect other functions and potentially the entire system. These functions are not a one-time process for a project, but are normally repeated many times during the project life cycle because the work product at various project stages may vary

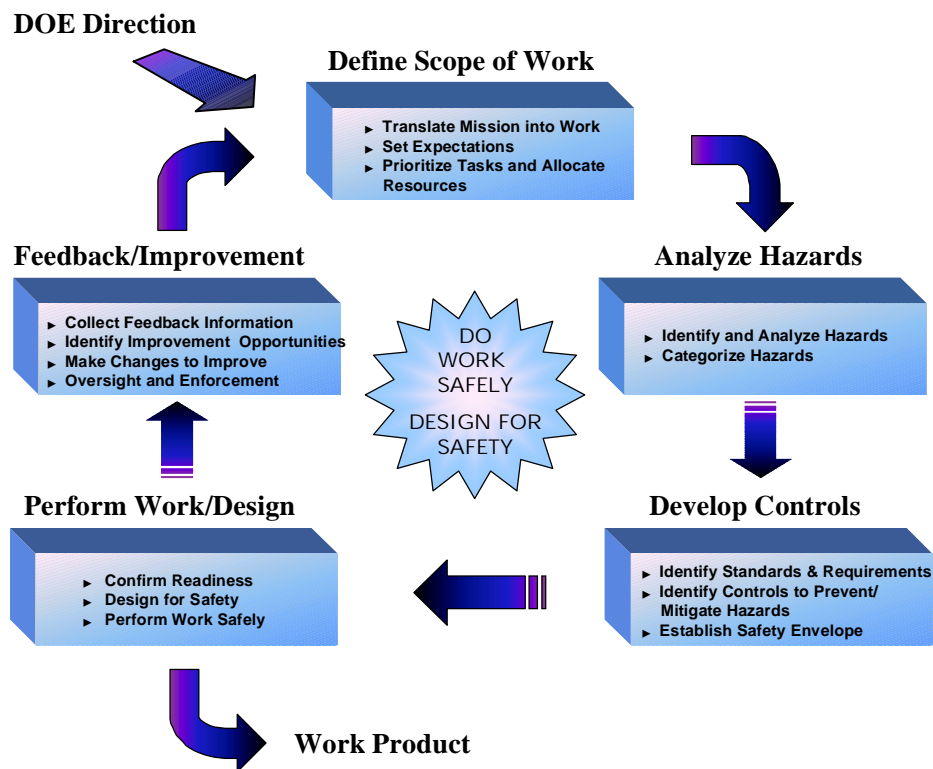


Figure 3-2. ISMS Functions

significantly. Addressing ISMS issues early permits a design-through-safety approach within the project. Thus, safety, health, environmental, and quality issues can be cost-effectively implemented in the design. Safety-through-design is not just meeting the specified safety requirements in the design. It is the project team taking specific actions regarding safety, and includes making design changes to: eliminate hazards, minimize hazards, mitigate consequences, and preclude the events that could release the hazard. Addressing hazards with a safety-through-design approach does not require that systems, structures, or components be added that will prevent or mitigate the releases. It involves removing or moving systems or adopting design approaches that result in a safer facility and improved operations, and often results in lower safety class and less safety significant controls being required in the final design.

For the simplest projects, the five core functions can be implemented in order. However, in projects involving a new design or significant modification, evolving design, or R&D, the project proceeds through the five core functions both at the project level and task level many times throughout the project life cycle. This relationship is presented graphically in Figure 3-3.

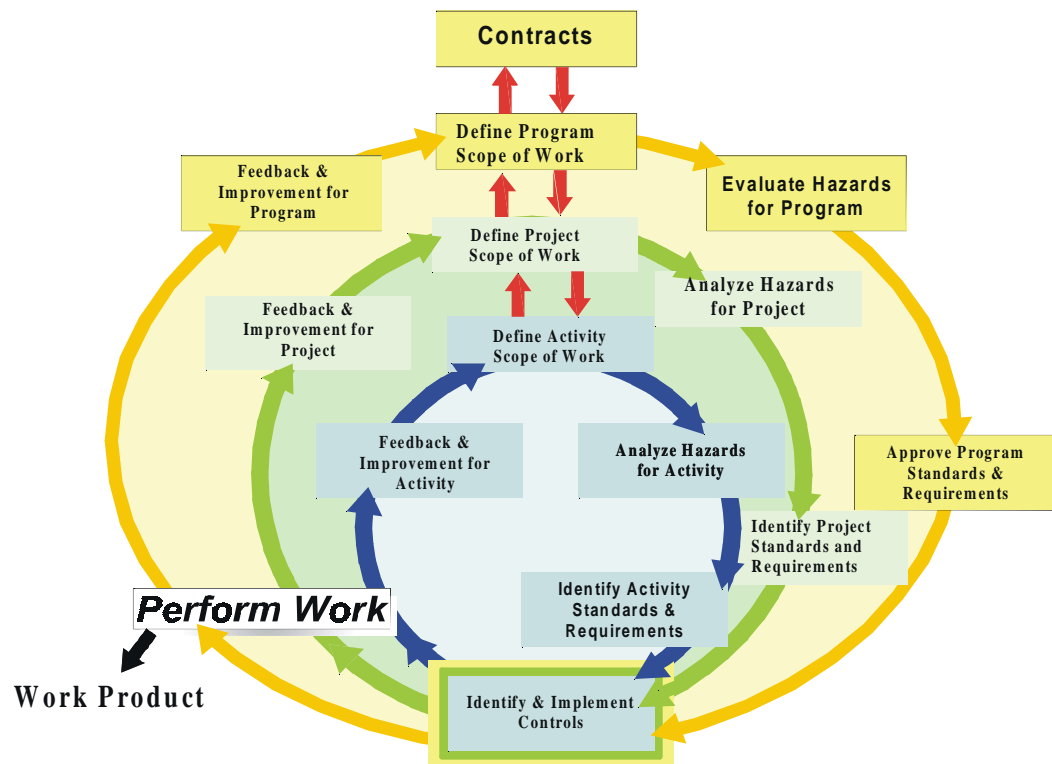


Figure 3-3. Relationship of ISMS Core Functions and Program, Project and Activity

It is important to note that the IPT may quickly move through each of the core functions many times in developing the conceptual design. The proper time to identify requirements, hazards, controls, potential solutions and the acceptability of the integrated set is early in the project life cycle. By approaching the design with a safety-through-design approach, the basic approach can be tested and the most appropriate solution defined. This may include challenging the reference design with innovative design solutions that change the basic processes to achieve a safe facility rather than just add controls to achieve safety. This approach of just changing the parameters to optimize the design has been used successfully by many projects to provide a significantly safer facility.

Baseline Scope of Work: During each design stage, the project documentation progressively develops more detailed requirements and project definition. The project requirements baseline and technical baseline form the basis for entering into the next project phase. This step creates the design baseline. It is important, early in the project, to evaluate the feedback provided in the fifth core function to determine the adequacy of the requirements and scope statement provided in this first core function. As the project moves to later stages of the design, then changes to the requirements and scope of work become more costly and need to be considered carefully as to whether the change is warranted.

Analyze Potential Hazards: Hazards and accidents are evaluated in progressively more detail as the design progresses from design stage to design stage. Although formal documentation of certain hazard analysis is not required until much later in the project, preliminary hazards and accident analysis should be initiated early to guide or drive design decisions and design requirements. It is important to identify the hazards and the potential release mechanisms associated with the hazards. This step provides guidance to those that develop controls and designs to safely handle the controls. This information can also be useful in providing feedback to the project as to the potential of eliminating or minimizing the hazard with reference design changes. The earlier in the project life cycle that these types of changes can occur, the more cost-effective the change.

Develop Design Controls/Requirements: The results of the hazard analysis and accident analysis provide input to the selection of applicable controls to assure that the facility meets all safety requirements. This element establishes requirements on the design that eliminates the hazard through design, minimizes the potential for events that could cause an uncontrolled release of the hazard, or provides controls that mitigate the consequences of an event that releases the hazard. Although project constraints, including applicable laws, rules, codes, and standards, are established for the overall project in the Define Scope of Work step, the detailed implementation and specific application of a law, rule, code, or standard is defined in this step.

Note that in addition to identifying physical and administrative controls, which will provide protection in the facility, the project needs to establish appropriate administrative design process controls to assure that: potential hazards have been addressed, appropriate stakeholders have provided input, the controls are adequate to provide the required function, and appropriate approvals have been provided to proceed to the next design step. These controls are established to provide the designer with the project requirements associated with seeking approval to continue within the Perform Work/Design element. The approval process is provided in the Feedback/Improvement element.

Perform Work/Design: This element is the creative function of the process where the architect/engineer produce a working design that will satisfy requirements, criteria, and other constraints from the previous element. The working design is assembled in project technical baseline documentation. These include documents such as the Facility Design Description and System Design Descriptions. These documents form the upper tier of the project's technical baseline and are therefore placed under configuration control. Specificity is added to these documents within each successive design phase.

Providing a design that meets the requirements and implements the controls identified in the previous function does not guarantee the best solution to providing a safe facility. The design process should adopt a safety-through-design approach to truly integrate safety into the design process. With designers participating on the IPT and in each of the previous functions, they are better able to understand the basis for the design requirements they are given. Additionally, this knowledge permits truly creative and innovative solutions to eliminating or mitigating hazards. The design team can therefore use the feedback core function to recommend changes that can lead to a more cost-effective solution to providing a safe facility.

Review, Feedback, Improvement and Validation: This element provides the review, feedback, improvement, and validation elements for the design. In general this function consists of both the scheduled and unscheduled design reviews. It includes top tier reviews such as the critical decisions, Safety Analysis Reports (PSAR, FSAR), and formal, independent project reviews. It also includes such lower-tier reviews as peer technical reviews of analysis and design, and early analysis feedback on design adequacy to meet identified safety requirements/controls. The review criteria and results from earlier stages are reexamined in each successive stage to ensure corrective actions from prior reviews have been taken and that changes have not invalidated results from earlier reviews.

3.2.3 Conceptual Design Stage Implementation

Figure 3-5 depicts the relationship between the ISM functions at the conceptual design stage of the project.

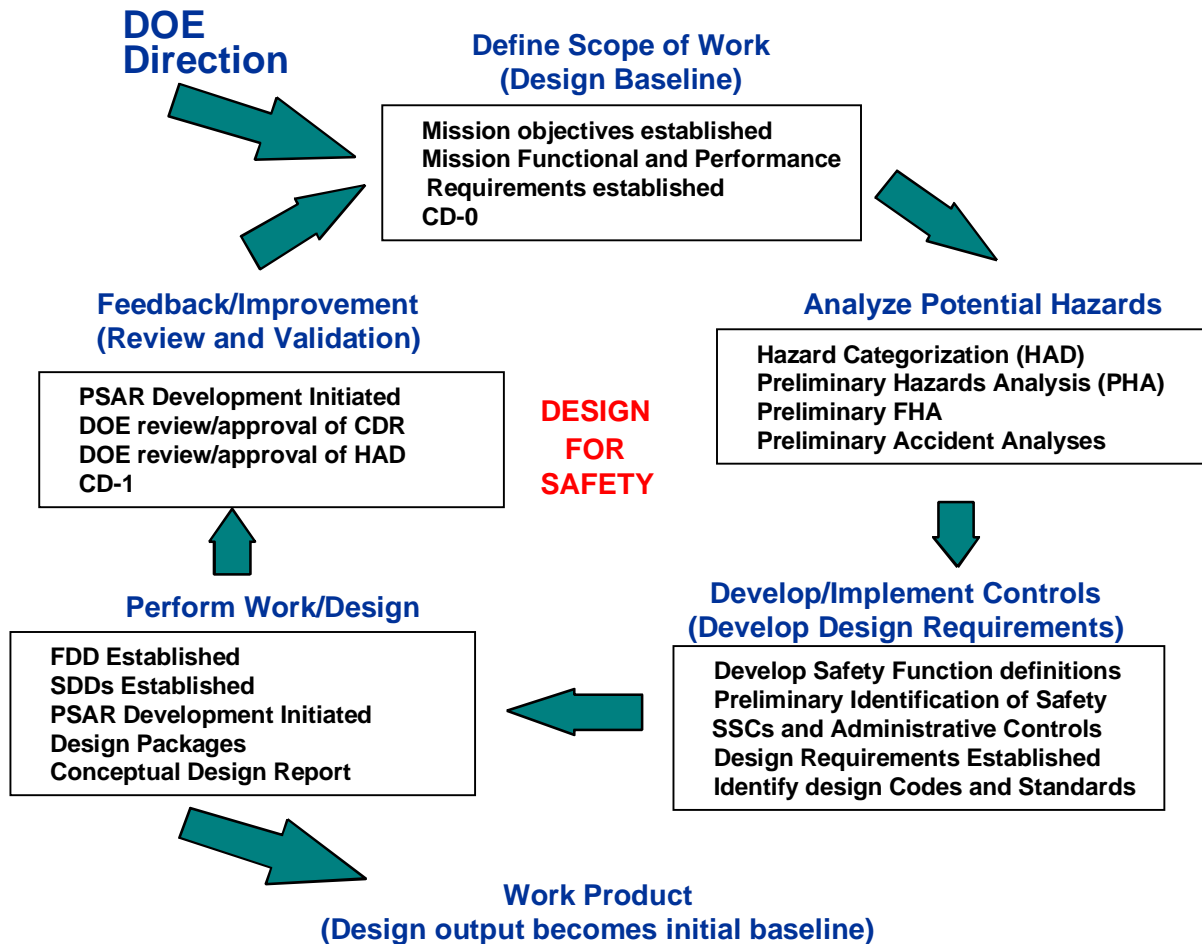


Figure 3-5. Conceptual Design Stage

Baseline Scope of Work:

Mission objectives are established. Once Critical Decision 0 is made, mission functional and performance requirements that will fulfill mission objectives are defined. These requirements form the definition of the design work to be performed during the conceptual design stage. It is imperative that the scope be defined enough to control the project, yet not over specify the design such that innovative solutions to providing safety are precluded.

Analyze Potential Hazards:

The requirements and guidance in this section supplements those in DOE O 420.1 and DOE G 420.1-1. Those two documents provide DOE's primary direction for the safety of nuclear facility design and modification.

For new nuclear facilities, a preliminary assessment of facility hazards is conducted based on a radiological inventory in accordance with DOE-STD-1027-92. For modifications to existing facilities, a similar determination based on inventory and process changes is needed. The results of this assessment are used to determine the initial hazard categorization for the facility and the level and type of safety documentation that will be required for the facility.

Building on the information collected during the initial hazard categorization and using the guidance on graded approach in DOE-STD-1027 and DOE-STD-3009, a Preliminary Hazards Analysis (PHA) is performed based upon envisioned inventories and processes. For hazard category 1 or 2 facilities, unmitigated accident scenarios are used to see if Safety Class structures, systems, and components are needed. Also, an initial set of Design Basis Accidents (DBAs) are identified for Category 1 and 2 facilities.

After the PHA is performed, the "final hazard categorization" is determined using the guidance in DOE-STD-1027. This categorization should be revisited periodically as the design evolves to ensure that the hazard category identified is still appropriate. It may be useful to determine whether certain design alternatives would result in the facility being in a different hazard category. If so, this could be a factor considered in the selection of design alternatives. Requirements for safety analysis and documentation are graded partly based upon the hazard categorization, using the guidance in DOE-STD-1027 and DOE-STD-3009.

A preliminary Fire Hazards Analysis (FHA) is performed for inclusion in the Conceptual Design Report to assure that appropriate attention has been paid to separation of structures, systems, and components and life safety egress considerations. In addition, early development of inputs the PSAR are initiated in this stage. It should be noted that within the ISM functions, the development of the PSAR serves several functions. The analysis required to develop the PSAR provides the information critical to the hazard analysis and the types of controls that are required to assure that the environment, public, and workers are adequately protected. It is a critical element of the Analyze Hazards step. Secondly, the analysis required to develop the PSAR may be used to select appropriate controls. Finally, it provides critical and timely feedback to designers regarding functions, design requirements, and acceptability of proposed design solutions.

Develop Design Controls/Requirements:

According to the requirements in DOE O 420.1 and the guidance in DOE G 420.1-1, decisions are made to reduce, prevent, or mitigate hazards. Alternative approaches should be considered and, if promising, carried further into the design process. As noted earlier in this section, the evaluation of alternatives should include not only alternative engineering controls, but innovative solutions that may eliminate or significantly reduce the hazard.

When prevention or mitigation is chosen, the preventive or mitigative functions required are developed into safety function definitions. Define programs guidance for safety function definition can be found in DP SIL 96-04. The ideal approach is to formulate the safety function definition independently and then, using the IPT and all appropriate stakeholders, identify or propose one or more structures, systems, and components that could best fulfill the function. During the conceptual stage, alternative design solutions should be identified and developed so that the optimal facility configuration can be chosen at CD-1. By involving applicable stakeholders in the selection of controls, the optimal facility configuration is developed as a part of the process and not as a stepping stone in the project lifecycle.

The end-product of this function is a preliminary identification of the structures, systems, and components that will be required to fulfill safety functions for the new or modified facility. In addition, alternative approaches are not only identified, but developed sufficiently to present as viable alternatives for CD-1. This important change to the way most DOE projects have been conducted in the past enables facility features and systems to be conceived and designed with safety-based requirements included and optimized, rather than added on later with attendant additional cost and decreased effectiveness.

During the conceptual design stage, safety function definitions are expanded and, using the hazard analysis results, developed into a general set of design requirements. For this stage, the design requirement parameters need only be developed sufficiently to use as a basis for estimating costs of major design features and components.

An important part of this process is the identification of codes and standards that will apply to the facility and its structures, systems, and components. During the conceptual design stage, the broadest identification includes laws, rules, regulations, DOE Orders, and DOE Guides; as well as building codes and industry standards having general applicability to the work to be performed.

Perform Work/Design:

Design output drawings for this stage should include facility layout and elevation drawings. Functional diagrams of important facility systems, including safety systems, should show system boundaries, major subsystems and components, interfaces to supported or supporting systems, and interfaces to other systems.

System Design Descriptions for safety structures, systems, and components are begun. The information described in Chapter 1 of DOE-STD-3024 is produced and placed under configuration control. The information described in Chapter 2 is prepared in draft. The information for the Facility Design Description that meets the intent of DOE-STD-3024 Chapters 1 and 2 is produced and placed under configuration control.

Review, Feedback, Improvement and Validation:

Feedback and Improvement is implemented in several layers within the project at each of the stages. PSAR development provides critical feedback to the project on requirements and acceptability of the proposed design solutions. PSAR development is therefore initiated in the conceptual design stage. In addition, task-level peer reviews, as well as formal project reviews, are implemented at this stage.

The following questions should be answered, if applicable to the project, during the conceptual design review process:

- ▶ Does the preliminary hazard analysis follow a methodology appropriate for the type of facility/process, the types of hazards that may be involved, and the level of analysis needed?
- ▶ Have all major types of hazards been addressed?
- ▶ Have forms and quantities of major hazardous materials been identified?
- ▶ Is there appropriate identification of all processes and operations?
- ▶ Are the safety function(s) defined in agreement with the define programs guidance in DP SIL 96-04?
- ▶ Have safety-class and safety-significant structures and systems been appropriately identified?
- ▶ Have design requirements for facility safety been preliminarily apportioned/assigned to identifiable systems or structures?

- ▶ Have the scope and boundaries of every safety system and structure been delineated?
- ▶ Have major subsystems and components, that may be associated with or defined as part of a specific safety system or structure, been preliminarily identified?
- ▶ Have major interfaces between safety systems and structures, and non-safety systems and structures, been preliminarily identified?
- ▶ Are major support and supporting systems preliminarily identified?
- ▶ Have political, strategic, and legal constraints on the safety design of the facility been identified?

3.2.4 Preliminary Design Stage Implementation

Figure 3-6 depicts the relationship between the ISM functions at the Preliminary Design stage of the project.

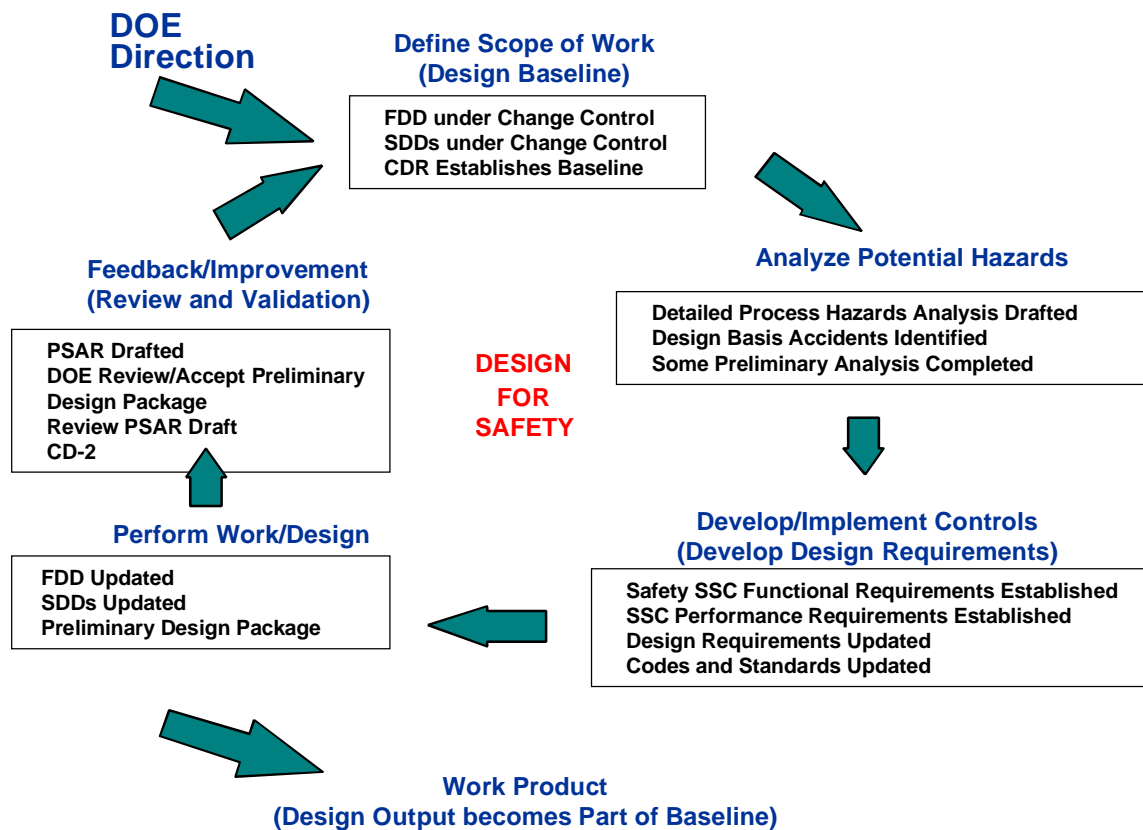


Figure 3-6. Preliminary Design Stage

Baseline Scope of Work:

The results of the Conceptual Design Report review establish the design baseline at the facility level and serve as the definition of technical work to be performed in the preliminary design stage. Those parts of the FDD and SDDs completed during the prior stage are placed under configuration control. Additional project constraints may be placed on the project based on the approval of the Conceptual Design Report. These constraints are included in project documentation.

Analyze Potential Hazards:

The results of the preliminary hazards analysis and the facility and process design from the previous stage are used as a basis for a more detailed process hazards analysis. Guidance for this analysis is provided in DOE-STD-1027 and DOE-STD-3009. Previous decisions on whether to reduce, prevent, or mitigate hazards are reviewed and modified as indicated.

For Category 1 and 2 facilities, the set of DBAs is finalized. DBAs are postulated accidents that the facility is designed to withstand. DBAs should be used to determine needed safety functions for safety structures, systems, and components. DBAs for a new facility are expected to result in negligible offsite consequences since the facility is designed to handle them.

Develop Design Controls/Requirements:

Alternative approaches that were identified during conceptual design are down-selected to the one (or, at the most, two) most promising to be continued in the design process. Safety systems are specifically identified and finalized following this down-selection. Safety function definitions from the previous stage are refined, if necessary, to reflect this increased specificity.

Design requirements for structures, systems, and components are updated to include functional requirements, specific parameters for performance, and the range of environmental conditions over which the structures, systems, and components is expected to fulfill its function. These requirements should fully support the fulfillment of identified safety functions.

The identification of laws, rules, regulations, DOE Orders, and DOE Guides; as well as building codes and industry standards that are applicable to the work to be performed; is taken to the next level by extracting (but preserving reference information) specific requirements that individual structures, systems, and components will comply with. Requirements that would be considered mandatory, but that will not be complied with, are also identified, and the basis for the noncompliance provided so that requests for exemptions or waivers can be prepared.

Perform Work/Design:

DOE O 420.1 provides the Department's requirements for the safe design of nonreactor nuclear facilities. DOE O 5480.30 provides the Department's requirements for the safe design of nuclear reactors.

The information described in chapter 2 of DOE-STD-3024 for SDDs is completed. The information for the Facility Design Description that meets the intent of DOE-STD-3024 Chapters 1 through 3 is completed.

Design output drawings for this stage should include system and facility layout and elevation drawings that indicate materials of construction. Also included are one-line diagrams for electrical systems, flow diagrams for ventilation systems, logic diagrams, and similar diagrams for other types of systems. Functional diagrams of important facility systems, including safety systems, should delineate system boundaries, show all subsystems and components, show interfaces to supported or supporting systems in detail, and show interfaces to other systems in detail.

Review, Feedback, Improvement, and Validation:

Review, feedback, improvement, and validation are implemented in several layers within the project at each of the stages. The PSAR development provides critical feedback to the project on requirements and acceptability of the proposed design solutions. The PSAR also provides a part of the basis for CD-2. A draft PSAR is therefore completed in the Preliminary Design stage. In addition, task-level peer reviews, as well as formal project reviews, are performed at this stage.

The following questions should be answered, if applicable to the project, during the Preliminary Design Review process:

- ▶ Does the hazard analysis (HA) process follow the guidance in DOE-STD-1027 and Chapter 3 of DOE-STD-3009-94?
- ▶ Is a recognized HA methodology used? For example, a methodology recommended in "Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples" from the Center for Chemical Process Safety.
- ▶ Is the methodology used appropriate for the type of facility/process, the types of hazards, and the level of analysis needed?
- ▶ Have all applicable types of hazards been addressed in the HA?
- ▶ Have all applicable release initiators been addressed (e.g., Internal/process, External, Natural Phenomena)?

- ▶ Have forms and quantities of all hazardous materials been identified?
- ▶ Are all processes and operations identified and clearly described?
- ▶ Have DBAs been identified and analyzed, as appropriate?
- ▶ Have appropriate safety-class structures and systems been identified?
- ▶ Have appropriate safety-significant structures and systems been identified?
- ▶ Are safety function(s) defined for each safety structure and system in agreement with the define programs guidance in DP SIL 96-04?
- ▶ Have all functions required for facility safety been apportioned/assigned to specific and uniquely identifiable systems or structures?
- ▶ Have the scope and boundaries of every safety system and structure been delineated?
- ▶ Have subsystems and components been associated with and defined as part of a specific safety system or structure?
- ▶ Have interfaces between safety systems and structures and non-safety systems and structures been identified and described?
- ▶ Are support and supporting systems identified?
- ▶ Are accidents, situations, and/or modes for which a system's or structure's safety function is required identified and linked to the safety analysis?
- ▶ Have appropriate sources for criteria-based requirements, specifically including DOE O 5480.30 or DOE O 420.1 and its associated Implementation Guides, been identified?
- ▶ Was a reasonable and complete set of criteria selected that encompasses applicable aspects of design and construction at an appropriate level?
- ▶ Is the extent and manner in which the selected criteria will be applied defined?
- ▶ Has the process by which design requirements will be developed and implemented from the selected criteria been defined?
- ▶ Has a set of functional requirements for each safety system and structure been defined?
- ▶ Are functional requirements referenced to the safety analysis?
- ▶ Do functional requirements support fulfillment of the system or structure's safety function?

- ▶ Are both active and passive functions identified?
- ▶ Have normal, abnormal, and accident conditions for which safety system and structures must fulfill their identified safety functions been estimated based on results of the safety analysis?
- ▶ Are plant or process parameters that need to be monitored as part of the operation of safety systems identified and understood?
- ▶ Are required plant, process, and system responses that are required as part of the operation of safety systems identified and understood?
- ▶ Does the decision on whether manual and/or automatic controls are provided reflect the results of safety analysis?

3.2.2.5 Final (Detailed) Design Stage Implementation

Figure 3-7 depicts the relationship between the ISM functions at the Final (Detailed) Design stage of the project.

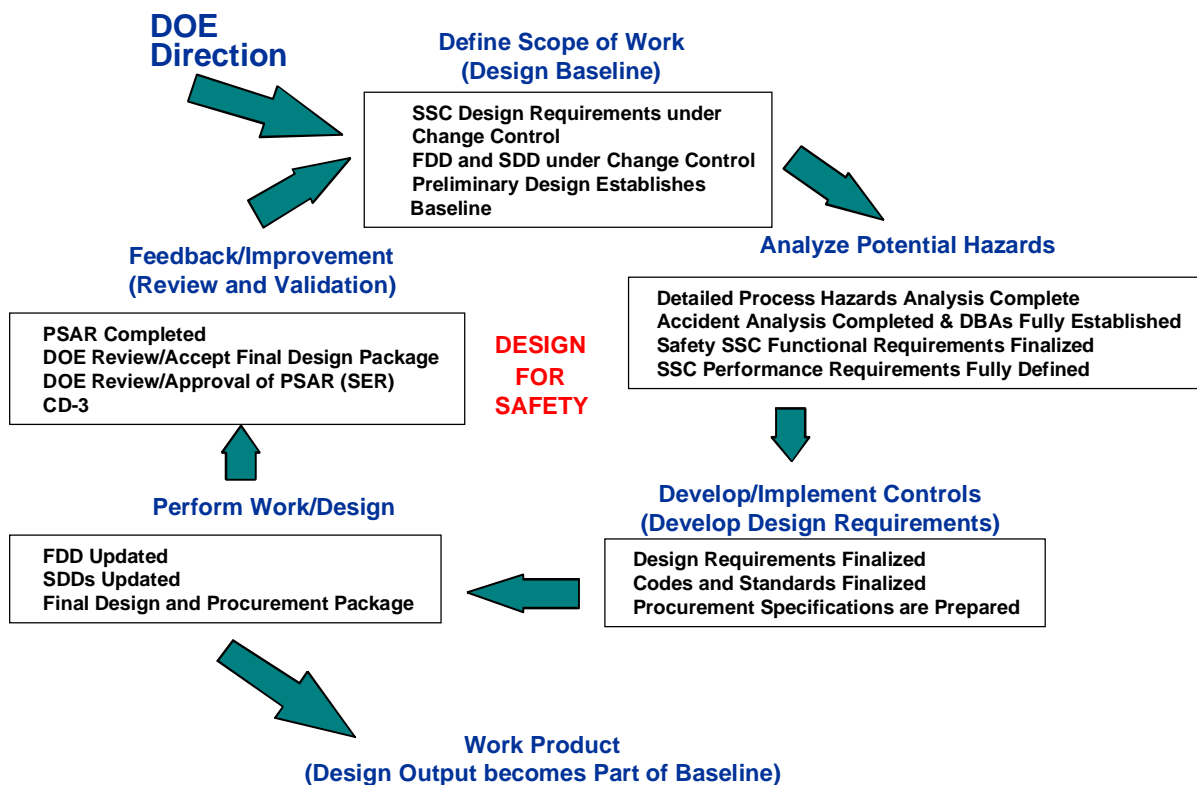


Figure 3-7. Preliminary Design Stage

Baseline Scope of Work:

Preliminary establishes the design baseline at the structure and system level, incorporating the results of the Preliminary Design Review. The design requirements for the facility and its structures, systems, and components are placed under change control. Those parts of the FDD and SDDs completed during the prior stage are placed under configuration control. Based on CD-2, additional constraints may be placed on the project by DOE. These controls should be included in project documentation.

Analyze Potential Hazards:

Before the detailed design of the facility can begin, all design requirements that will be generated from safety considerations should be known. Therefore, all analyses that will appear the PSAR need to be completed early in Final Design. A detailed process hazards analysis, based on the preliminary process design is completed according to DOE-STD-3009. Accident analyses are completed based upon final definitions of design basis accidents. The information described in Chapter 2 of DOE-STD-3024 for SDDs is completed. The information described in Chapter 3 is prepared in draft. The information for the Facility Design Description that meets the intent of DOE-STD-3024 Chapters 1 through 3 is completed.

The hazards and accident analyses provide the basis for finalization of the functional requirements of facility structures, systems, and components. Performance requirements for all structures, systems, and components can then be fully defined. Performance requirements are acceptance criteria or limits against which the actual performance capability of the as-built system will be evaluated.

Develop Design Controls/Requirements:

The information described in Chapter 2 of DOE-STD-3024 for SDDs is completed. The information described in Chapter 3 is prepared in draft. The information for the Facility Design Description that meets the intent of DOE-STD-3024 Chapters 1 through 3 is completed.

The results of the preceding function are combined with other design requirements and specific requirements from codes and standards to finalize the design requirements for structures, systems, and components.

At this point, enough information is known about major systems and components to prepare the technical inputs for procurement specifications. Safety analysts, designers, and purchasing managers work together to ensure that important design features and parameters will appear in procurement documents when they are issued.

Perform Work/Design:

The information described in Chapter 3 of DOE-STD-3024 for SDDs is “finalized” and placed under configuration control. The information for Chapter 4 is prepared in draft, describing systems as the construction, startup/turnover package will portray them. The Facility Design Description is completed and placed under configuration control. The detail design package and Final Design report are prepared.

Review, Feedback, Improvement, and Validation:

Review, feedback, improvement, and validation are implemented in several layers within the project at each of the stages. The PSAR development provides critical feedback to the project on requirements and acceptability of the proposed design solutions. The PSAR provides the basis for the DOE SER and also provides a part of the basis for CD-3. The PSAR is therefore completed in the Final Design stage. In addition, task-level peer reviews, as well as formal project reviews, are performed at this stage.

The following questions should be answered, if applicable to the project, during the Final (Detailed) Design Review process:

- ▶ Has a set of appropriate accident types been identified and characterized?
- ▶ Have DBAs been identified and analyzed, as appropriate?
- ▶ Have criteria-based requirements been refined and successive tiers of referenced criteria been incorporated?
- ▶ Are safety structures, systems, and components and their associated support systems designed to standards and quality requirements commensurate with their importance to safety?
- ▶ Are the designs of safety systems adequate to fulfill their identified functional requirements?
- ▶ Are safety structures, systems, and components designed so they can be expected to perform their safety function reliably under those conditions and events for which their safety function is intended? Is the facility and its systems designed to perform all safety functions with the reliability indicated by the safety analysis?
- ▶ Do the designs of safety systems comply with identified criteria-based requirements?
- ▶ Are safety structures, systems, and components designed to withstand all design basis loadings, with an appropriate margin of safety?

- ▶ Is all equipment selected for application to the specific service conditions based on sound engineering practices and manufacturers' recommendations.
- ▶ Does the facility design provide reliable safe conditions and sufficient confinement of hazardous material during and after all DBAs?
- ▶ At both the facility and structures, systems, and components level, does the design ensure that more probable modes of failure (e.g., fail to open versus fail to close) will increase the likelihood of a safe condition?
- ▶ Are the identified quality assurance provisions commensurate with the structures, systems, and component's importance to safety?

3.2.6 Construction, Startup/Turnover Stage Implementation

Figure 3-8 depicts the relationship between the ISM functions at the Construction, Startup/Turnover stage of the project. As construction, testing, and startup are included in this stage, ISM implementation for physical work (construction, testing, startup, etc.) becomes significant, in addition to the safety-through-design implementation evident in the previous stages.

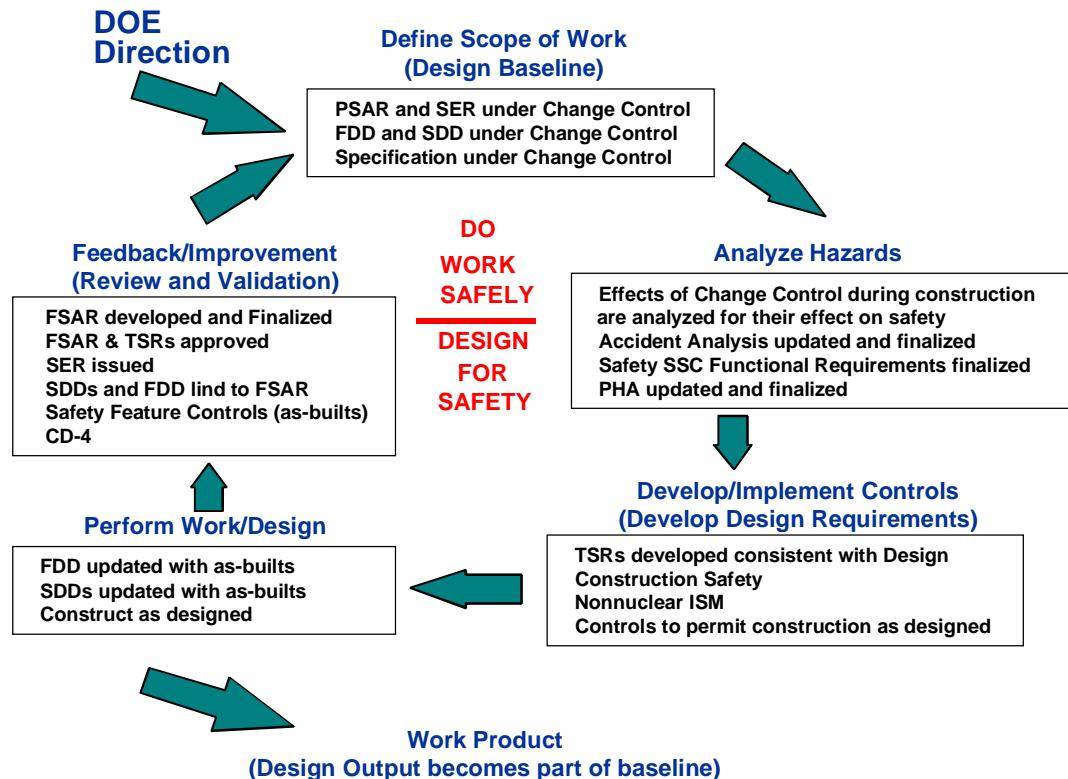


Figure 3-8. Construction, Startup/Turnover

Define Scope of Work:

The design baseline includes construction drawings. The PSAR is approved and its SER written. Both documents are placed under configuration control. The detailed design, including the FDD and SDDs, is placed under configuration control. These documents, and the Final Design Report, define the facility to be constructed during this stage.

Analyze Hazards:

The effects of changes made during construction are analyzed to ascertain their effect on the approved PSAR, and are reviewed and approved at predefined levels. In addition to the potential hazards of facility operation, the hazards associated with construction, testing, and startup must be evaluated.

Develop/Implement Controls:

During construction, component specifications are issued and are used as the technical requirements for procurement of the components and subsystems that will comprise the major structures, systems, and components. Controls associated with construction, testing, and startup must be implemented, based on the hazard analysis.

Perform Work/Design:

SDDs are completed and placed under configuration control. The FDD is updated as indicated and remains under configuration control. Construction, testing, and startup tasks are completed. Once the facility is built, as-built drawings, an approved FSAR, and its SER are required for CD-4.

Review, Feedback, Improvement and Validation:

Review, feedback, improvement, and validation is implemented in several layers within the project at each of the stages. The FSAR development provides critical feedback to the project acceptability of the final design solutions. The FSAR provides the basis for the SER and a part of the basis for CD-4. The FSAR is therefore completed in the Construction, Startup/Turnover stage. In addition, task-level peer reviews, as well as formal project reviews are performed at this stage.

The following questions should be answered, if applicable to the project, during the Construction, Startup/Turnover review process:

- Is the FSAR approved?

- ▶ Has the SER been issued?
- ▶ Do SDDs and the FDD properly link to and support the FSAR?
- ▶ Do as-builts identify safety features?

3.2.7 Summary of ISM Implementation in Design

Figure 3-9 summarizes the ISM design stage expectations for each of the five core functions. By following this approach, and implementing a safety-through-design approach, a project can be accomplished with high confidence that all aspects of safety have been included into facility design. The transition between design and operations should also proceed smoothly since the safety analysis products have been integrated by the IPT with the design and planned operations integrated with the design and reflect the as-built facility. The alignment of the operating procedures and practices, safety documentation, and the physical configuration are maintained in alignment with a working configuration whose physical systems fall with a working configuration management program.

3.2.8 Worker Protection

The primary focus of worker protection during the design phases of a project is: (1) providing a design that limits the hazards for which workers are exposed and (2) providing a design with specific items credited with providing protection for workers, and (3) a robust design based on defense in depth. Traditional worker protection issues handled by integrated safety management are included in all physical facility work practices including construction, testing, inspection, and associated R&D activities. Programs and practices for field work is adequately addressed within both DOE guidance and DOE site practices and will not be address further in this manual. Two examples of these worker protection programs and practices, which are implemented within ISM, are presented in Figure 3-10 for the Voluntary Protection Program (VPP) and in Figure 3-11, Enhanced Work Planning (EWP).

Figure 3-9. Summary of ISM Expectations by Design Stage

ISM Function	Integrated Safety Management Design Steps at each Stage of the Acquisition Sequence			
	Conceptual Design	Preliminary Design	Final Design	Construction, Startup/ Turnover
Define Scope of Work (Design Baseline)	<ul style="list-style-type: none"> • Mission Objective Established • Mission Functional and Performance Requirements Established • CD-0 	<ul style="list-style-type: none"> • FDD under Change Control • SDD under Change Control • CDR Establishes Design Baseline 	<ul style="list-style-type: none"> • SSC Design Requirements • FDD and SDD under Change Control • Preliminary Design Report Established Design Baseline 	<ul style="list-style-type: none"> • PSAR and SER under Change Control • Detailed Design under Change Control • FDD and SDDs under Change Control
Analyze Potential Hazards	<ul style="list-style-type: none"> • Hazard Categorization • Preliminary Hazard Analysis • Preliminary Fire Hazards Analysis 	<ul style="list-style-type: none"> • Process Hazards Analysis • Design Basis Accidents Identified 	<ul style="list-style-type: none"> • Detailed Process Hazard Analysis Complete • Accident Analysis Completed and DBAs Fully Established 	<ul style="list-style-type: none"> • Effects of Changes during Construction are Analyzed for their Effect on Safety • PHA Updated and Finalized • Accident Analysis Updated and Finalized
Develop Design Controls/Requirements	<ul style="list-style-type: none"> • Develop Safety Function Definitions • Preliminary Identification of Safety SSCs • Design Requirements Established • Identify Design Codes and Standards 	<ul style="list-style-type: none"> • Safety Functions Finalized • Identification of Safety SSCs Complete • Safety SSC Functional Requirements Updated • Codes and Standards Updated 	<ul style="list-style-type: none"> • Safety SSC Functional Requirements Finalized • SSC Performance Requirements Fully Defined • Design Requirements Finalized • Codes and Standards Finalized 	<ul style="list-style-type: none"> • TSRs Developed Consistent with Design • Construction Safety Controls Defined and Implemented
Perform Work/Design	<ul style="list-style-type: none"> • FDD Established • SDDs Established • Conceptual Design Report 	<ul style="list-style-type: none"> • FDD Updated • SDDs Updated • Preliminary Design Package 	<ul style="list-style-type: none"> • Procurement Specifications Prepared • FDD Updated • SDDs Updated • Final Design Package 	<ul style="list-style-type: none"> • Construction Safety following ISM Implementing Program • FDD Completed • SDDs Completed • As-Built Developed
Review, Feedback, Improvement and Validation	<ul style="list-style-type: none"> • PSAR Development Initiated • DOE Review/Approval of CDR • CD-1 	<ul style="list-style-type: none"> • Draft PSAR Established • DOE Review/Approval of Preliminary Design Package • CD-2 	<ul style="list-style-type: none"> • PSAR Complete • DOE Review/Approval of Final Design Package • CD-3 	<ul style="list-style-type: none"> • FSAR Developed and Finalized • DOE Review/Approval of FSAR (SER) • FDD, SDDs, As-Built as Controlled Documents that Control Safety Features • Confirm Readiness to Operate • Transition to Operations • CD-4

Figure 3-10. ISMS Functions Crosswalk with VPP Elements

<div>ISMS</div> <div>VPP</div>	Scope of Work	Analyze Hazard	Develop/Implement Controls	Perform Work	Feedback Improvement
Management Leadership	+Annual Operating Plan	+Line Management Responsible for SARs	+Line Management Responsible for TSRs	*Line Management Approvals	*Management Walkdowns *Management Evaluations
Employee Involvement	*Fix it Now Teams *Work Management Centers *Shift Turnovers	*JHA Procedure *Fix it Now Teams *Work Management Centers +PHR	*JHA Procedure *Fix it Now Teams *Work Management Centers	*Stop Work Authority *Fix it Now Teams *Work Management Centers	*Fix it Now Teams *Work Management Centers *Employee Concerns Program *Safety Observers *Critiques *Green Cards
Worksite Analysis		+SAR +PHR *PHA *JHA +USQ			
Hazard Prevention and Control					
Safety and Health Training	+Annual Operating Plan Training		+S/RID Training	+Conduct of Operations Training	+Expanded Root Cause Analysis Training

Legend: + ISMS only in red; * Both in blue; - VPP only in green; No matches expected in gray areas

Figure 3-11. ISMS Functions Crosswalk with EWP Elements

ISMS EWP	<u>Scope of Work</u>	<u>Analyze Hazards</u>	<u>Develop/Implement Controls</u>	<u>Perform Work</u>	<u>Feedback Improvement</u>
Line Management Ownership	*Work Management Centers	*Work Management Centers	*Work Management Centers	*Work Management Centers *Line Management Approvals	*Mgmt Walkdowns *Mgmt Evaluations
Organizationally Diverse Teams	*Fix-it-Now Teams *Work Management Centers	*Work Management Centers +PHR Teams	*Work Management Centers	*Fix-it-Now Teams *Work Management Centers	*Fix-it-Now Teams
Graded Approach	*Fix-it-Now Teams *Work Management Centers	*JHA Procedure *Fix-it-Now Teams *Work Management Centers	*Work Management Centers +Equipment Functional Categorization	*Work Management Centers *Fix-it-Now Teams	Grading provided within programs listed in this column
Worker Involvement	*Fix-it-Now Teams *Work Management Centers *Shift Turnover	*JHA Procedure *Fix-it-Now Teams *Planner Pre-job Walkdowns *Work Management Centers	*JHA Procedure *Fix-it-Now Teams *Work Management Centers	*Stop Work Authority *Fix-it-Now Teams *Work Management Centers	*Fix-it-Now Teams *Work Management Centers +Employee Concerns Program +Safety Observers +Green Cards
Organized Communication					+Mgmt Evaluations +FEB Visits

Legend: +ISMS only in red; *Both in blue; -EWP only in green; No matches expected in gray area

3.3 SAFETY

3.3.1 Safety Implementation Detailed Planning

TABLE OF CONTENTS

List of Effective Pages

List of Figures

List of Tables

Acronyms

1 Introduction

1.1 Purpose and Scope

1.2 Safety Philosophy

2 Integrated Safety Management Implementation

2.1 Safety Goals and Requirements

2.2 Overall Facility Safety Objectives

3 Safety Requirements

3.1 Safety Design Requirements

3.2 Construction Safety Requirements

4 Safety Basis

4.1 Hazard Analysis

4.1.1 Hazard Categorization

4.1.2 Hazard Analysis

4.2 Accident Analysis

4.3 Safety Controls

4.3.1 Classification of Safety Functions

4.3.2 Selection of NPH Performance Categories

4.3.3 Technical Safety Requirements

4.4 Safety Analysis Documentation

4.4.1 Preliminary Safety Analysis Report (PSAR)

4.4.2 Final Safety Analysis Report (FSAR)

5 Construction Safety

6 Configuration Management

7 Independent Review

7.1 Safety Analysis Report Independent Review

7.2 Final Safety Analysis Report Independent Review

7.3 Operational Readiness Review

8 Schedule

Appendix A. Review of DOE Order 5480.23: Applicability to PSARs

Appendix B. Applicability of DOE-STD-3009-94 to PSAR

Figure 3-12. Safety Implementation Planning Document

Safety implementation planning is an extremely useful communication tool for developing safety documentation. An example safety implementation planning document outline is presented in Figure 3-12. The primary purpose of this plan is to document the lower-level safety documentation development schedule and communicate the level of safety documentation that will be available at each stage of the project.

The Safety Implementation Detail Planning document contains the definitive statement of the project safety philosophy, objectives, top-level safety requirements, and basis for each safety document that will be developed for the project. The more complex the facility and the longer the project schedule, the more important the safety implementation plan becomes. For example, no definitive guidance is provided for the contents of a Preliminary Safety Analysis Report or a Limited Work Authorization. Therefore, the safety detailed planning document provides the regulators with the communication tool containing the detail that will be available for review at each critical decision point. This documentation could be as simple as identifying the PSAR chapters that would be developed or as complex as providing a description of the level of detail that will be provided in each section of the PSAR, based on the outline of the FSAR as contained in DOE STD 3009.

Thus, the Safety Implementation Detailed Planning document allows the project to document its graded approach to developing the safety documentation based on the hazard category of the facility and the overall complexity.

3.3.2 Safety Requirements

Safety requirements are controlled in the FDD and specific SDDs. For complex facilities, a single document may be beneficial in which all safety requirements are captured and controlled. In this case, a safety requirements document could be useful. The purpose of developing a safety requirements document is to provide documentation of safety-driven requirements and goals, as well as the basis for each. This would include the top-level design requirements based on the hazard and processes within the facility. It would also include derivative requirements that are based on the specific design solutions to safety functions and the requirements derived from the design basis accident analysis demonstrating acceptability of the design solutions. It is important not to include requirements handled by national consensus codes and standards within this document, but only include those requirements driven by development of the facility authorization basis.

The safety requirements document is primarily a project tool used by safety professionals to document the breadth of the safety requirements in a single location. The implementation of these requirements in design and operation is via the Facility Design Description and System Design Descriptions. It provides a centralized location for safety professionals to document requirements that flow from the safety analysis, along with the bases for each requirement. This facilitates transfer into the applicable system design descriptions and the Facility Design Description as appropriate. The requirements should be developed and documented according to system or subsystem (i.e., by the System Design Description). Additionally, the function (safety classification that the requirement is helping to satisfy) should be captured. The function may be captured as a part of the requirement development or as a part of the basis for the requirement. Additionally, the highest safety classification (functional classification—Safety Class, Safety Significant, or lower-tier classification) that the requirement is helping to satisfy should also be documented in either the basis or with the requirement.

3.3.3 Authorization Basis Documentation

Authorization basis documentation development should be initiated early in the conceptual design stage. The hazard analysis document, developed in accordance with DOE-STD-1027 determines the level of safety documentation that is required for the project and facility. In addition, the Preliminary Hazard Analysis will provide input to the definition of Design Basis Accidents (DBAs) and the extent of accident analysis that will be required to complete the safety documentation. Other than providing feedback and in some cases driving design and design requirements, the development of the safety case can lead to additional safety documents being required. If the construction schedule is extremely long (for example, caused by long-lead material requirements), then a Limited Work Authorization (LWA) may be required for DOE to authorize limited construction activities (including early procurement). This permits construction activities or procurement of long-lead materials to be initiated prior to approval of the PSAR.

As no specific DOE guidance has been provided to cover a Limited Work Authorization, it is imperative that the plans be delineated in the safety implementation plan and approved by DOE. Critical to the acceptability of the LWA is demonstrating that the significant issues have either been addressed or that remaining issues are not affected by the LWA, making the risk to DOE for moving forward acceptable.

The stages of SAR development are described in the various design stages described in Section 3.2 of the Practices. Note that with integration of the safety

documentation task and the design tasks, the SAR becomes a managed report that is issued at decision points (or based on an annual update) to document the current status of the safety case for the facility. Thus managed, the PSAR is developed to the point of turnover and DOE acceptance, the PSAR becomes the FSAR with minimal project impact or delays.

3.3.4 Safety Evaluation Report

The DOE project manager or ES&H manager should develop a plan to review the authorization basis documentation and prepare the Safety Evaluation Report (SER) for the project. The safety review plan should be updated for each project stage to define the level of review that will be applied for the next critical decision. The SER is developed consistent with the requirements of DOE-STD-1104 “DOE, Review and Approval of Nonreactor Nuclear Facility Safety Analysis Reports.” An example Safety Review Plan outline is presented in Figure 3-13. Critical elements of the Safety Review Plan are the schedule, staffing, review guidelines, method of documenting comments, and method of closure on comments. Overall, the Safety Review Plan should also define the expectations for the safety documentation and the purpose of the review. Thus, this would change for each project stage.

3.3.5 Unique Aspects of Projects Modifying Existing Facilities

In general, the principles associated with developing a safety case and supporting a modification to an existing facility and a greenfield facility are effectively the same. However, there are unique aspects associated with a modification that need to be highlighted to assure that adequate attention is paid to them by the project.

3.3.5.1 Develop and Define Objectives and Safety Scope of Modification

Whether or not a modification is specifically intended to affect the safety of facility operations, there is always a desire to use the opportunity to improve the safety design of the facility. This desire should be effectively balanced against available funding and schedules. The existing facility safety basis should be consulted and any new hazards identified and analyzed. During conceptual design, additional or improved safety controls should be proposed and ranked according to safety benefit and cost. Use safety design criteria as part of the input for identifying the range of improvements that could be made—like fixing single failure points, seismically-upgrading, providing backup power, failing to preferred mode, etc.

Figure 3-13. Example Safety Review Plan Outline

CONTENTS	
1. INTRODUCTION	
1.1	Purpose
1.2	ISRC Organization and Staffing for the PSAR and SER
1.3	PSAR Basis
1.4	PSAR Review Basis (Scope of the Review)
1.5	SRP Organization
2. SAFETY OBJECTIVES AND THE ROLE AND EXPECTATION OF THE PSAR	
2.1	PSAR Review Planning Considerations
3. ANTICIPATED PRODUCTS	
4. INTERFACES WITH OTHER APT DEVELOPMENT ACTIVITIES AND REVIEW TEAM ORGANIZATION	
4.1	Interfaces with Other Development Activities
4.2	Technical Independent Review Organization
5. ASSUMPTIONS	
6. TECHNICAL APPROACH TO THE PSAR REVIEW	
7. PSAR REVIEWS	
7.1	Resources
7.2	Review Orientation
7.3	Documentation of Comments
7.3.1	Levels of Comments
7.3.2	Format and Content of Comments
7.4	Review Process
7.5	PSAR Review Guidelines
7.5.1	Accident Analysis
7.5.2	Site Characteristics and Cleanup Chapters
7.5.3	Programmatic Chapters
8. LIMITED WORK AUTHORIZATION	

9. SER PREPARATION AND ASSIGNMENTS

- 9.1 SER Preparation Team Organization
- 9.2 Process for Identifying SER Issues
- 9.3 Review Guidelines to be Used in the SER
- 9.4 SER Preparation, Review, and Approval Process
- 9.5 Quality Assurance Requirements for the Preparation of the SER
- 9.6 SER Content and Format Guidance

10. MILESTONE SCHEDULE

11. PROFILES OF PSAR REVIEW AND SER PREPARATION PARTICIPANTS

12. RECORD KEEPING

13. REPORTS

- 13.1 Meeting Minutes
- 13.2 Formal Technical Evaluations
- 13.3 Informal Technical Evaluations
- 13.4 Periodic Progress Reports
- 13.5 Draft SER

14. REFERENCES

Appendix A—Definitions

Appendix B—PSAR Content Expectation and Safety Review Guidance

Appendix C—Independent Review Process

During preliminary design, safety controls that will be provided should be identified and justified. Controls that were proposed but not selected should be justified.

This approach can provide the greatest safety benefit possible within funding limits. With a clearly defined and justified project scope, the “ratchet effect” (when outside project reviewers try to get everything fixed under the sponsorship of the project) can be answered with a technically defensible justification.

3.3.5.2 Fund and Schedule Safety Analyses and Review in Project Plan

In addition to the analyses discussed elsewhere in this section, the existing FSAR will need to be updated to reflect the modification, and DOE will need to complete an SER. These efforts can require significant effort and time, but should be managed as tasks within the project so that they will incur a minimal impact on project cost and schedule.

3.3.5.3 Understand Effects of Changes

New or revised analyses should identify the effects of proposed changes on facility safety. Available design documents and safety basis should be researched to understand why the facility is the way it is (or why it is not the way it appears it should be). Special attention is necessary to make sure that changes will not violate any previous assumptions or restrictions. Consider new hazards that will be introduced, and how existing hazards are affected. Determine whether the hazard categorization of the facility will change. Determine whether any systems will change their safety classification.

A second project decision is likely to be required based on the review of existing documentation. If the facility is new or has undergone design basis reconstitution to document the technical baseline in a Facility Design Description and System Design Description, then the documentation for the facility should be adequate and the project will be modifying existing documentation. However, if the facility is lacking good technical baseline documentation, then a decision will be required as to the depth of design basis reconstitution that the project wants to or is required to fund in order to provide adequate documentation for the project. This should be performed on a graded approach based on facility resources. The facility modification project can not be encumbered by the second project to reconstitute the facility baseline. Only that portion of the facility that is being modified is required to be captured in updated technical baseline documents. However, the project could use the Facility Design Description/System Design Description development process to begin the baseline reconstitution process.

3.3.5.4 Obtain DOE Review and Approval of Safety Aspects of Change

An unreviewed safety question determination should not be done, because DOE must always approve major modifications to existing facilities. But the same analyses is done, analyzing the safety of the changed facility. New or revised analyses should be started during the conceptual phase and updated during each phase. The difference between existing and proposed safety should be highlighted. DOE reviews and approves the analyses. At the end of the project, the FSAR is updated to capture the change and DOE provides an SER.

If the facility has a Facility Design Description and System Design Description, then documentation of the change is easily tracked via the revisions of affected documents. If the Facility Design Description and System Design Descriptions are not available, then as a minimum a change package should be prepared that depicts affected portions of the facility both before and after the modification. This will help preserve a record of the facility configuration that is important for analyzing future changes. In addition, sometimes changes cause unforeseen problems that can only be remedied by restoring the original configuration.

3.3.5.5 Compare Codes and Standards for the Existing Facility to Current Codes and Standards

New construction generally conforms to current codes and standards. With modification work, there may be some conflict between the codes and standards that the existing facility conforms to and the current codes and standards.

During the conceptual design phase, codes and standards that apply to the work are identified according to the Integrated Safety Design process and approved by DOE. During the preliminary design phase, research and review of the existing design baseline includes identification of the codes and standards originally applied to the construction of the existing facility. Past modifications may also have incorporated codes and standards that are different from the original construction. The report on the preliminary design phase should document a comparison of existing versus current and identify how differences will be resolved. The preliminary design report should specifically indicate which baseline codes and standards will continue to apply, where codes and standards will be updated, and what new codes and standards will be applied.

3.3.5.6 Account for Changes to the Loading of Support Systems

Evaluate whether the modification will increase or decrease loading of support systems. Identify existing margins and spare capability that may be depleted. Identify existing redundant support systems and determine whether redundancy will be maintained. Identify any support systems that will require modification to increase capacity, preserve redundancy, or provide new redundancy. Evaluate and properly preserve interfaces between new or modified systems and existing systems, paying special attention to interfaces between safety and non-safety structures, systems, and components.

The impact on support systems is one of the reasons for involving all stakeholders in project planning. Before the project is initiated, the complete impact on the facility and site infrastructure needs to be identified. Impacted systems or organizations (such as fire protection) may need to change existing programs or procedures to accommodate the design modification. Lead times for infrastructure upgrades at existing facilities could be the driving factor in the overall project schedule.

3.3.5.7 Ensure Safety During Modification Work

Apply traditional Integrated Safety Management practices to the planning associated with performing physical work and the execution of the construction phase of the modification. Unique aspects of modification work that may require special attention include maintaining the integrity of existing confinement barriers, protection of construction personnel from existing nuclear hazards, and whether credible construction accidents are bounded by the facility's existing safety basis.

3.4 ENVIRONMENT

The International Standards Organization (ISO) 14001 has been used by many sites and projects to implement an environmental management system as required by Executive Order 13148. The Executive Order does not require compliance with ISO 14001, however the principles contained in ISO 14001 can serve as the central framework for the environmental management system (EMS) required by the Order. Due to the number of sites implementing or gaining certification in the standard, the EMS will be discussed in terms of the standard. An EMS is composed of the elements of an organization's overall management structure that address the immediate and long-term impact of its products, services, and processes on the environment. An EMS provides order and consistency in organiza-

tional methodologies through the assessment of environmental impacts, assessment of legal and regulatory requirements, allocation of resources, assignment of responsibilities, and ongoing evaluation of practices, procedures, and processes.

The environment includes the surroundings in which an organization operates. This includes water, air, land, natural resources, flora, fauna, humans, and their interrelation. Environmental requirements, documentation, and implementation are integrated into the project programs and overall schedule via the Project Execution Plan. The method for implementation is via the ISMS described in this section of the Practices and in Section 3 of the manual.

3.4.1 Requirements and Guidance

Environmental management processes are required by Executive Order 13148, "Greening the Government through Leadership in Environmental Management" and discussed in DOE G 450.4-1A, "Integrated Safety Management System Guide." The environmental baseline for the project is established prior to any work being performed at the site. For ER projects, the environmental baseline is typically provided as an integral part of the baseline risk assessment. Implementation of the required environmental management system may be through compliance with or certification against ISO 14001, "Environmental Management Systems—Specification with Guidance for Use." The project EMS may be part of a larger site-wide EMS or for a new greenfield project that is not on an existing DOE site, developed only for the project.

The project should be implemented under a written environmental management process in order to anticipate and meet growing environmental performance expectations and to ensure ongoing compliance with national and international regulatory requirements. This could be a site process or one developed specifically for the project.

In general, if an organization is going to implement an ISO 14001 environmental management system, the management program should achieve the following:

- ▶ Assess potential environmental impacts.
- ▶ Assess legal and regulatory requirements.
- ▶ Establish an appropriate lifecycle environmental policy, including a commitment to prevention of pollution.
- ▶ Determine the legislative requirements and environmental aspects associated with the project activities, products, and services.

- ▶ Develop management and employee commitment to the protection of the environment, with clear assignment of accountability and responsibility.
- ▶ Encourage environmental planning throughout the full range of the organization's activities, from raw material acquisition through product distribution.
- ▶ Establish a disciplined management process for achieving targeted performance levels.
- ▶ Provide appropriate and sufficient resources, including training, to achieve targeted performance levels on an ongoing basis.
- ▶ Establish and maintain an emergency preparedness and response program.
- ▶ Evaluate environmental performance against the policy and appropriate objectives and targets, and seek improvement where appropriate.
- ▶ Establish a management process to review and audit the EMS and identify opportunities for improvement of the system and resulting environmental performance.
- ▶ Establish and maintain appropriate communications with internal and external interested parties.
- ▶ Perform a senior management review of the system to ensure that the process remains effective.
- ▶ Encourage contractors and suppliers to establish an EMS or other type of written environmental management process.

Environmental considerations are part of most projects, regardless of the project type (e.g., modification, construction, environmental cleanup, facility startup). Environmental planning is needed early in each project's planning stage to avoid delays and ensure compliance with applicable regulations. Projects for federal agencies are often subject to more regulations than for commercial projects. In addition, compliance actions for environmental regulations often invoke specific time frames and/or a sequence of process steps. Examples include obtaining a Resource Conservation and Recovery Act (RCRA) permit or completing the National Environmental Policy Act (NEPA) process, which involves issuing such documents such as Records of Decision (RODs) and Findings of No Significant Impact (FONSI). It is important for the project management team to understand the regulatory framework for the various environmental regulations—particularly those associated with environmental cleanup. The typical steps each project needs to complete to ensure it meets its environmental stewardship commitment are outlined in Section 3.2 of the manual.

3.4.2 Environmental Management System (EMS)

The environmental aspects of the project should fit within the EMS for the site. Note that if the project is not located on a DOE site with an existing EMS, a site EMS needs to be developed for the project. The five elements of EMS defined in ISO 14001 are:

- ▶ Policy
- ▶ Planning
- ▶ Implementation and Operation
- ▶ Checking and Corrective Action
- ▶ Management Review.

The elements of the EMS can be compared to the five core functions of the ISMS as described in Figure 3-14. Although there is not a one for one comparison of the elements of the EMS with the ISM core functions, the key aspects of each are embodied in the other. In effect the EMS establishes boundaries for performing work based on the potential impact on the environment. Implementation though the ISMS provides specificity to the middle element of the EMS (Implementation and Operation), when the work is actually performed.

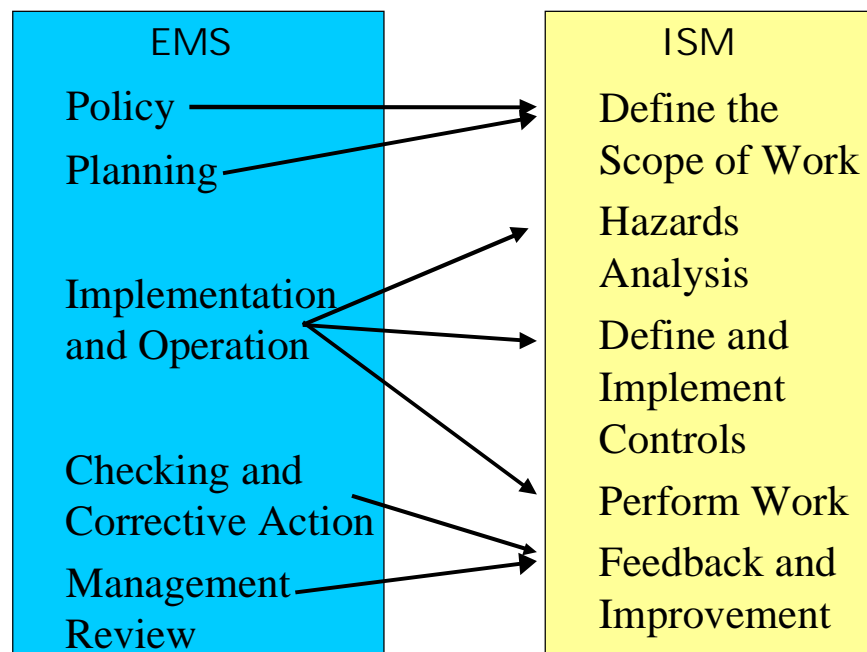


Figure 3-14. EMS / ISM Element Comparison

An example outline of an EMS and activities flow chart are presented in Figure 3-15.

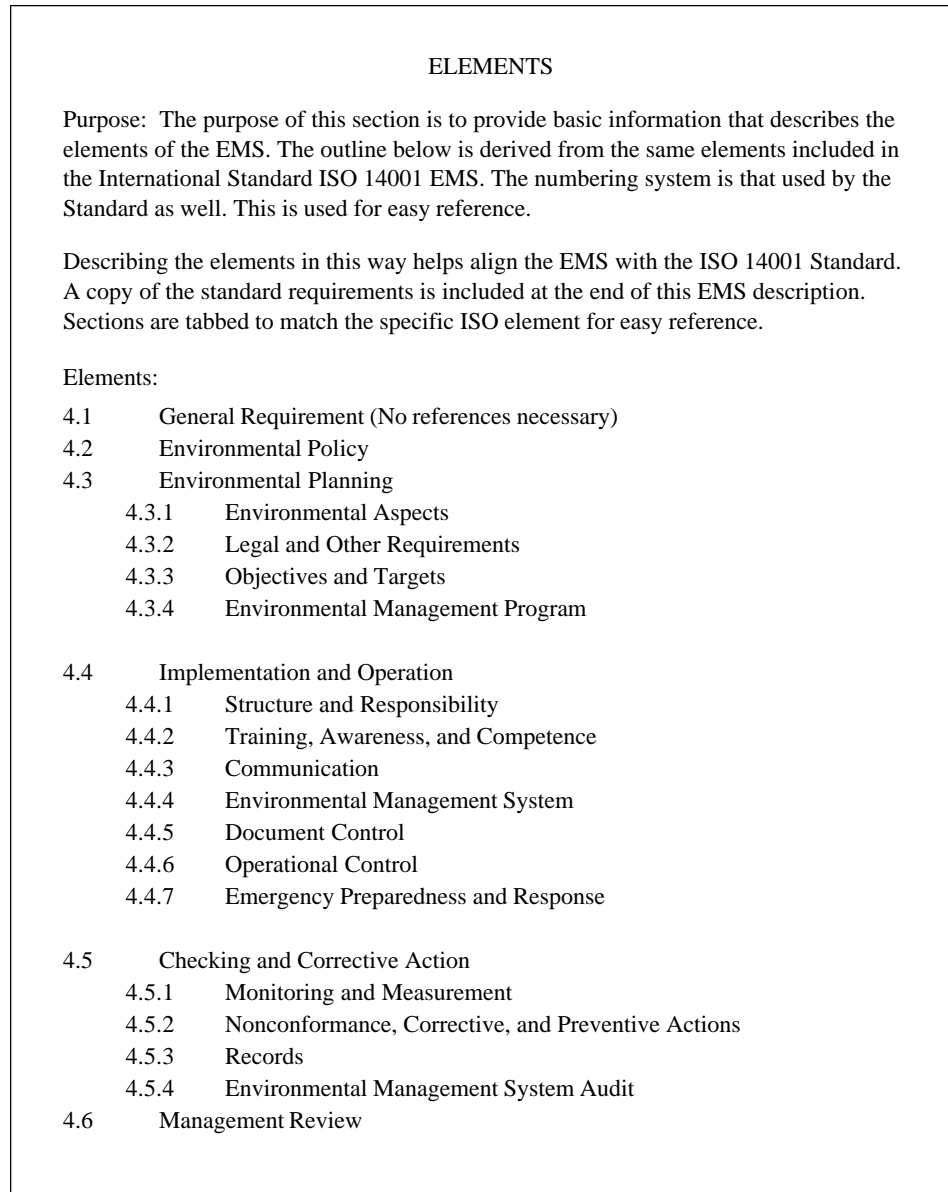


Figure 3-15. Example EMS Outline and Related Documentation

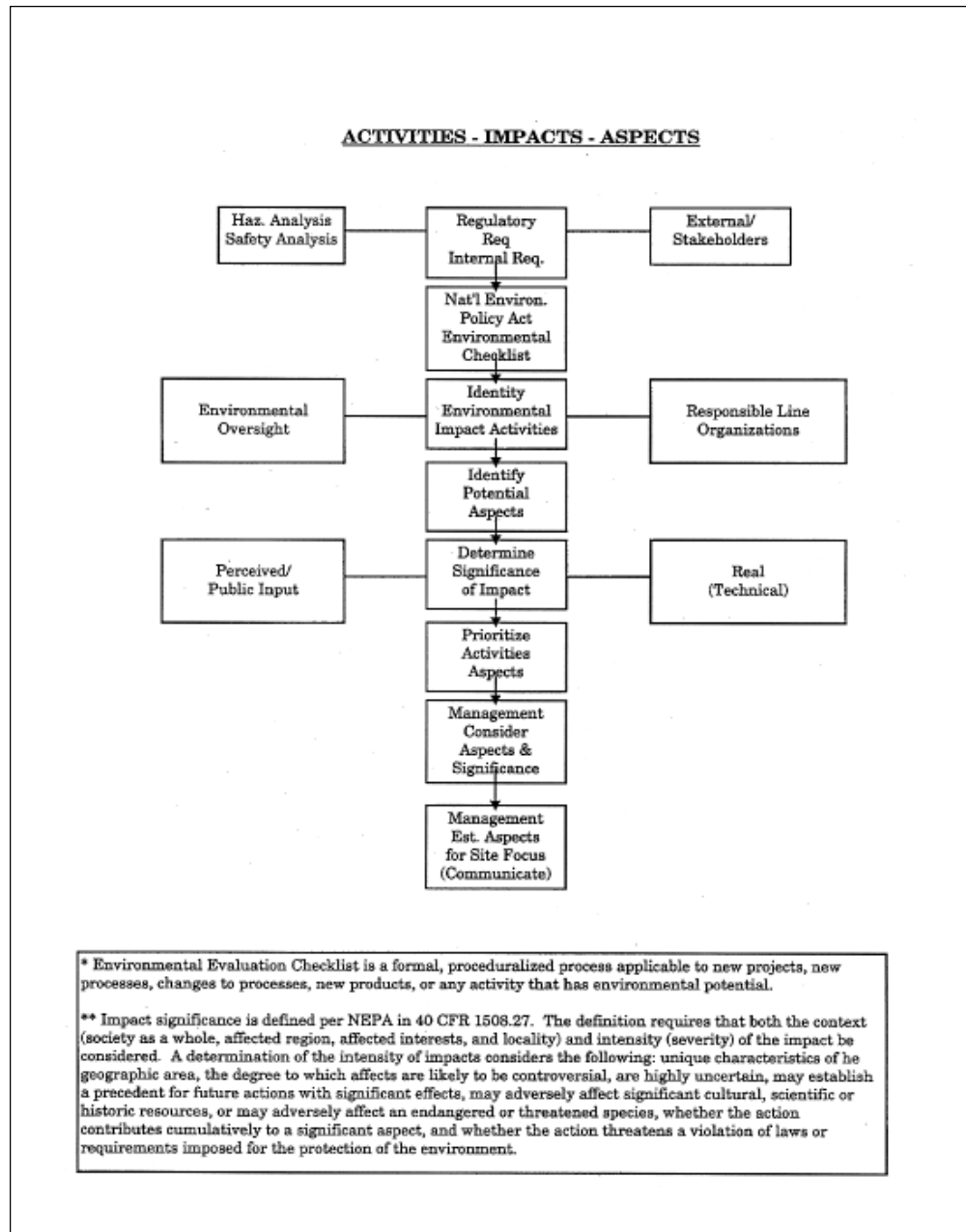


Figure 3-15 (continued)

Preliminary environmental evaluations typical of a major project are organized as shown in Figure 3-16. Although a time line is assumed from the figure, no unique time line can be assumed. The purpose of this figure is to provide a visual depiction of the types of documents and/or activities that should be applied and the type of information included in the documentation.

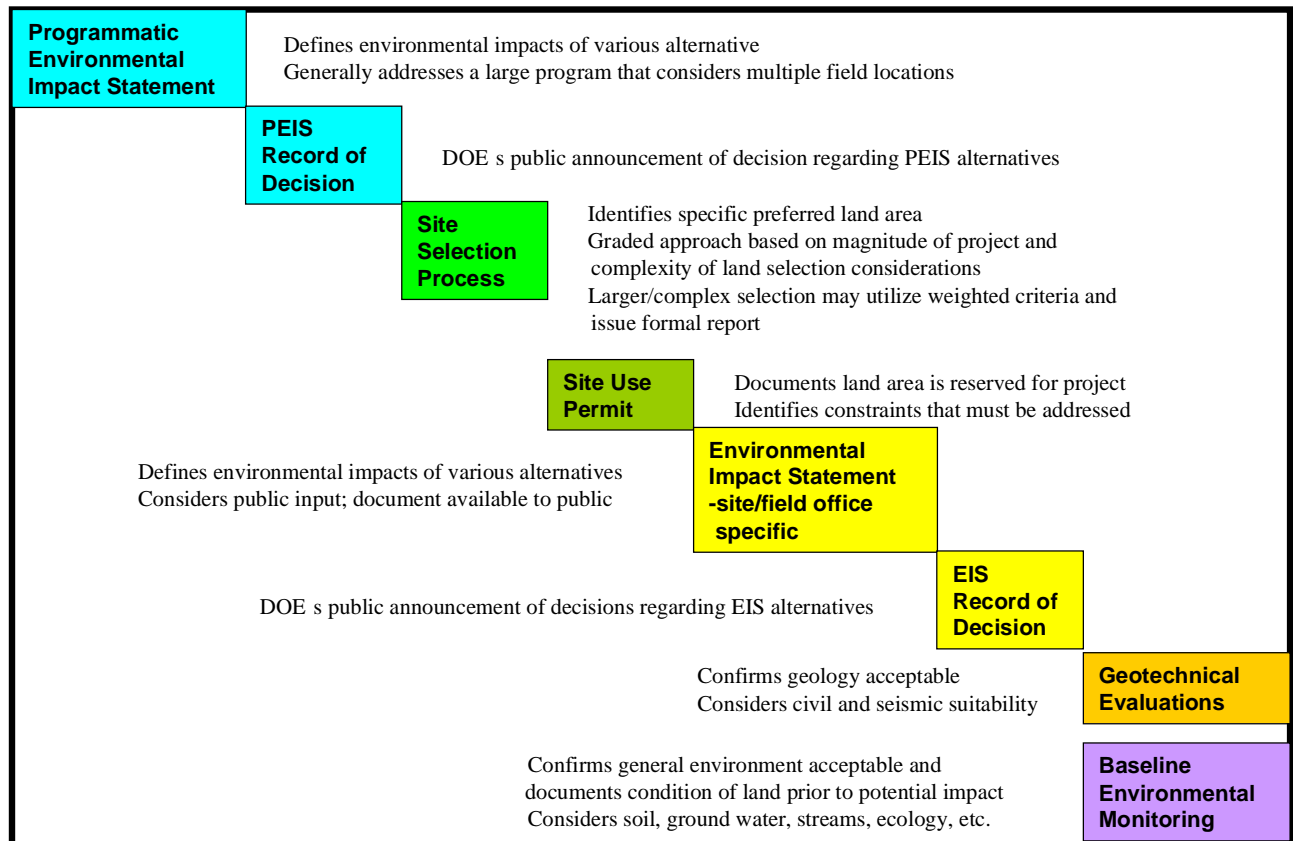


Figure 3-16. Project Preliminary Environmental Evaluation

To assure that an ISO 14001 EMS is adequately implemented in the ISMS, a crosswalk between the existing ISO 14001 and the ISM requirements is beneficial. A typical example is depicted in Figure 3-17.

Figure 3-17 ISMS Function Crosswalk with ISO 14001 Elements

ISO 14001 \ ISMS	Scope of Work	Analyze Hazards	Develop/Implement Controls	Perform Work	Feedback Improvement
Policy	*EMS Policy		*Policy Manual *Environmental Management Council *EMS Policy		
Planning	*Strategic Plan *Annual Operating Plan *Waste Management & Pollution Prevention Plans	*NEPA Procedure *Environmental Monitoring Plan *Aspect Determination	*S/RID or Work Smart Standards		
Implementation & Operations			*Environmental Compliance *Operations *Management Req'ts and Procedures *Quality Assurance *Compliance Assurance	*Facility Specific Procedures *HAZMAT, HAZCOM, & Waste Handling Training	
Checking & Corrective Actions			*Records Management		*Performance Metrics *NCRs *EMS Audit *Effluent monitoring
Management Review					*Mgt Review Requirements *EMS Man Review Procedure *Citizens Advisory Board

Legend: +ISMS only in red; *Both in blue; -EWP only in green; No matches expected in gray area

3.5 QUALITY

3.5.1 Introduction

Quality Assurance is a tool to be used by the project manager to provide a level of assurance that the project is meeting the customer's requirement. Beyond that, nuclear and environmentally significant (regulatory driven) projects impose quality requirements to provide a basis for stating that the regulatory requirements (nuclear or environmental) have been met.

Whether the selected standard has 10 (414.1) or 18 plus 4 supplements and 3 appendices (RW-0333P), all quality programs are focused on providing the structured system that defines the control features that will demonstrate through objective evidence that the project requirements have been met. These control features are for the most part good business practices. These features document the design, have it reviewed, and have the changes controlled. Similarly, they describe the organization of the project and the quality-affecting activities. In summary, the quality program's function describes the extent the project will control all of the key aspects such as organization, design, procurement, documents, records, inspection, testing, defects, maintenance and test equipment, and the process the project will use to review these aspects and make sure the control features continue to function as planned.

3.5.2 Quality Assurance Plans (QAPs)

In a general sense, the more risk involved in the project the more control is needed. As an example, Appendix 1 provides a matrix of the procedure to meet the requirements for compliance with the Office of Civilian Radioactive Waste Management (OCRWM), Quality Assurance requirements, and descriptions for Radioactive Waste Management (DOE RW-0333P). The project implementing documents section provides a general listing of the organizations, including QA, that need to have documented methods for meeting the customer-mandated requirements for the Civilian Radioactive Waste Management Program.

Appendix 2 provides a matrix of typical project procedures needed to define a quality program that will meet the requirements of 10 CFR 830.120.

Appendix 3 provides a table of contents for a quality assurance plan that describes how the project will meet the requirements of either DOE Order 414.1A or 10 CFR 830.120.

Appendix 4 provides an index of quality assurance procedures that would typically be prepared to meet the requirements of a nuclear project that must comply with 10 CFR 830.120 and has selected ASME NQA-1 as the industry standard to follow. Supporting procedures from other organizations such as engineering, procurement, records, testing etc. would all show up in the matrix (Appendix 3) attached to the QA Plan for the project. This set of procedures provides the control system for the project to assure that the customer's requirements for the project will be met. It takes all of the project participants to make this happen.

3.5.3 Quality Program Tailoring and Categorization

The description in Section 3 and appendices provide a view of very detailed programs with all the elements essential for control of high-risk, potentially significant environmental or radiological activities. The determination of the impact on project mission, safety and the environment of any activity is required early in order that appropriate controls can be instituted to minimize the potential for significant issues occurring. As the risk of injury or insult reduces, the controls can also be reduced. Another aspect that is also considered when categorizing systems or items is the potential impact to project cost or schedule.

Significance Categorization:

The project should develop a list of items and activities as early as possible and determine the significance of the item or activity to the success of the project. Things that should be considered in assigning significance include:

- a) Radiological or Industrial Safety to the public and worker
- b) Potential to impact the environment
- c) Potential to impact the acceptability to the customer (Can you prove it is good?)
- d) Potential to impact project completion date
- e) Potential to impact project cost
- f) Regulatory significance
- g) Public perception
- h) Others

Once the significant discriminators for the project items or activities are determined they can be used to apply the appropriate level of review and oversight.

For example, in low-level radioactive waste shipments, the radiological hazard is low, the customer acceptance needs are high, and the public perception (if waste is spilled on the highway) is significant. Therefore one would expect to apply a significant effort to assure that the shipping containers and DOT shipping requirements are met. This typically would include independent inspection of the procurement and receipt integrity of the containers, independent verification of the radiological conditions, and an independent verification that the loaded containers meet the DOT shipping requirements for placards, manifest, and such.

Another example, is the high-level vitrified waste being prepared for storage in a federal repository. The quality requirements for the chemicals that are used to manufacture the waste are limited to the process controls necessary to assure that when the chemicals are mixed with the waste, the resulting mixture will produce a vitrified waste that complies with the repository requirements so that high-level waste quality program requirements are not applied to the chemicals.

Quality Program Tailoring

Quality program tailoring is accomplished by applying only those quality program elements to an item or activity that are required to accomplish the goal of having an item or activity meet the mission needs and customer requirements.

The key is to having trained and qualified quality personnel with a sound technical background who can understand both the quality program requirements and the important technical aspects of the project activities.

Categorization usually is used to determine the need to apply quality program controls. Once the need to assign a level of assurance is determined, the description and extent of this assurance should be a mutual agreement between the quality organization and the technical organization. Typically, the responsible engineer and the quality engineer will discuss the item or activity and reach a conclusion on the appropriate level of oversight needed to assure the acceptability of the item or activity for the project. Factors that enter into the determination include:

Items

- a) Will the item be contaminated in use?
- b) Can the item be removed or repaired?
- c) Will the item cost the project money or affect the schedule if it is procured incorrectly?

- d) Are the dimensions important to it's function?
- e) Is the material important?
- f) Does the customer requirements dictate specific needs?
- g) Others.

Activities

- a) Does the activity require independent oversight (e.g., for safety or project Requirements)?
- b) Is a record required that the activity was performed correctly?
- c) Other.

In some cases, project or customer requirements will include specific action be taken such as receipt inspection of all procured items or vendor qualification for all items that are fabricated to project design.

All of these decisions and activities associated with selecting the appropriate quality requirements for an item or activity are part of the specific tailoring of project quality requirements to the circumstances and require knowledgeable and experienced people in the quality assurance organizations as well as the technical organizations. Tailoring is the tool that the project uses to minimize the quality cost for the project by applying appropriate controls based on risk.

This page is intentionally blank.

Practice 4

Project Execution Plan

